THE CLAIMS AS HEREIN AMENDED

1. (canceled)
2. (canceled)
3. (canceled)

4. (currently amended) A method of conducting electronic credit card transactions so as to guard against fraud, comprising the following steps:

using a computer program mandated by a credit card issuer, ~~an internet browser~~ a user of a credit card issued by the ~~a~~ credit card issuer (a) initiates a proposed credit card transaction with a third party vendor by accessing via said third party vendor a party authorized by said credit card issuer to validate credit card transactions, and (b) transmits ~~and transmitting~~ to said authorized party ~~credit card~~ non-encrypted information concerning the user and an encrypted personal identification number that comprises in encrypted form a date/time stamp and certain information identifying said user ~~identifying said user and an encrypted date/time stamp representing the current transaction time~~ ;

said authorized party receives said encrypted personal identification number ~~date/time stamp~~ and said non-encrypted ~~other credit card~~ information and decrypts said encrypted personal identification number to derive said date/time stamp and said certain information identifying said user ~~stamp to derive the current transaction time as represented by said decrypted date/time stamp~~ ;

said authorized party (1) compares said ~~credit card~~ non-encrypted and decrypted information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized user and (2) also compares the current transaction time represented by said decrypted date/time stamp with the time of its receipt of said encrypted date/time stamp

and determines if the difference, if any, between said times is within a predetermined time limit; and

depending on the determination made in the foregoing step, the authorized party communicates to said third party vendor either a validation or rejection of the proposed transaction.

5. (canceled)
6. (canceled)
7. (canceled)
8. (canceled)
9. (canceled)
10. (canceled)

11. (currently amended) A method for authorizing an electronic business transaction by an authorized user, comprising the steps of:

(a) storing information about authorized users~~, including pre-set public key numbers and private key numbers for each authorized user,~~ in a validating system~~, and providing said public and private key numbers to said authorized users for use in initiating and completing electronic transactions~~;

(b) receiving in the validating system for verification an encrypted time-limited personal identification number ~~code~~ which is transmitted in connection with a proposed electronic business transaction at the request of a person who may or may not be an authorized user, said encrypted personal identification number ~~code~~ comprising an encrypted date/time stamp ~~representing the time that the proposed electronic business transaction was initiated by said person,~~ and certain encrypted user-identifying information ~~a public key number and a private key number~~;

(c) decrypting said received encrypted personal identification number ~~code~~ to retrieve said date/time stamp and said certain encrypted user-identifying information~~, said public key number and said private key number~~;

(d) comparing said decrypted certain user-identifying information with the authorized user information ~~decrypted public and private key numbers with the pre-set unique public and private key numbers~~ stored in said validating system to verify that said decrypted certain user-identifying information is valid ~~that they are valid~~, and rejecting the proposed transaction if said decrypted certain user-identifying information is ~~said decrypted public and private key numbers are~~ not valid; and

(d) if said decrypted certain user-identifying information is ~~said decrypted public and private key numbers are~~ verified as valid, (1) determining from said decrypted time stamp if the age of the proposed transaction is within a predetermined time limit required for validating the transaction ~~comparing the time represented by said decrypted date/time stamp with the time of receipt of said transmitted encrypted code by said validating system~~, and (2) rejecting the proposed transaction if the age of the proposed transaction is not within said ~~there is a difference between the time represented by said decrypted date/time stamp and said time of receipt, and that difference exceeds a~~ predetermined time limit.

12. (currently amended) The method of claim 11 wherein said electronic transaction is a credit card transaction, and said certain user-identifying information comprises ~~public key number is~~ a credit card account designation.

13. (currently presented) The method of claim 11 wherein said encrypted code received by said validating system is transmitted to said validating system via a third party vendor, and further wherein rejection or authorization of said proposed transaction is communicated by said validating system to said vendor.

14. (canceled)

15. (canceled)

16. (currently amended) The method of claim 11 wherein said encrypted personal identification number ~~code~~ includes a public key and a private key ~~an encrypted PIN~~.

17. (canceled)

18. (canceled)

19. (canceled)

20. (currently amended) A method of limiting the amount of time information pertaining to a credit card issued by a credit card issuer is valid for use in support of an electronic transaction with a vendor comprising the following steps:

A. a credit card user records credit card information required by the vendor ~~via an internet browser~~, including credit card number, credit card expiration date, and the name of the credit card user;

B. said user uses a computer program provided by the credit card issuer or a party acting on behalf of said credit card issuer to provide ~~generates~~ a date/time stamp representing the current date and time and to generate an encrypted personal identification number that comprises ~~encrypts~~ said date/time stamp and at least some of said recorded credit card information;

C. said encrypted personal identification number is ~~date/time stamp and said encrypted credit card information are~~ transmitted from said credit card user via said vendor to a party authorized by the credit card issuer to validate proposed credit card transactions;

D. said party authorized by said credit card issuer to validate proposed credit card transactions conducts a validation process that

comprises: (1) decrypting said encrypted personal identification number to retrieve said date/time stamp and said at least some recorded ~~date/time stamp and said encrypted~~ credit card information, (2) determining from said decrypted date/time stamp if the age of the proposed transaction ~~as represented by the time of the decrypted stamp~~ is within a predetermined time limit required for validating the transaction, (3) comparing said decrypted credit card information with previously recorded credit card user information to verify that the party initiating the proposed credit card transaction is an authorized credit card user, and (4) depending on the determinations made in foregoing steps (D)(2) and (D)(3), communicating either a validation or rejection of the proposed transaction to the third party vendor and/or the party who initiated the proposed credit card transaction.

21. (canceled)

22. (previously presented) A method according to claim 20 wherein step B includes encryption of said credit card number.

23. (currently amended) A method for conducting credit card transactions so as to guard against fraud, said method comprising steps as follows:

(a) a credit card user who proposes to carry out a credit card transaction with a third party vendor initiates the transaction by accessing a computer program supplied by the credit card issuer or a party acting on behalf of said credit card issuer that is constructed so as to (1) obtain a date/time stamp from a time source and (2) generate a time-limited personal identification number for the credit card user by encrypting ~~encrypt~~ said date/time stamp and certain required credit card information identifying the ~~a~~ credit card user;

(b) said credit card user supplies said certain required credit card information to said computer program and said computer program (a) obtains a date/time stamp ~~in response to said certain credit card information~~ and (b) generates ~~an encrypted~~ a personal identification number ~~code~~ comprising said date/time stamp and said certain required credit card information in encrypted form;

(c) said ~~encrypted~~ personal identification ~~code~~ number comprising said date/time stamp and said certain required credit card information in encrypted form is transmitted via said third party vendor to a validating system authorized to validate credit card transactions on behalf of said credit card issuer;

(d) said validating system decrypts said ~~encrypted~~ personal identification code to derive the ~~current transaction~~ time as represented by said ~~the~~ decrypted date/time stamp and also said certain required credit card information ~~in decrypted form~~ ;

(e) said validating system (1) compares said decrypted certain required credit card information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized credit card user and (2) also compares the current transaction time represented by said decrypted date/time stamp with the time of its receipt and determines if the difference, if any, between said times is within a predetermined time limit; and

(f) depending on the determinations made in foregoing steps (e)(1) and (e)(2), the validating system communicates either a validation or rejection of the proposed transaction to the third party vendor and/or the party who initiated the proposed credit card transaction.

24. (previously presented) A method according to claim 23 wherein said certain required information includes a credit card number and/or a private key number.

25. (currently amended) A method according to claim 23 wherein said computer program is installed on ~~the credit card user's~~ a computer containing a browser, and step (c) is conducted via the internet using said browser.

26. (previously presented) A method according to claim 23 wherein said computer program is installed on a remote server and is accessed by said credit card user.

27. (currently amended) A method for conducting electronic transactions so as to guard against fraud, said method comprising steps as follows:

(a) an entity who wishes to carry out an electronic transaction with a bank initiates the transaction by accessing a computer program supplied by said bank that is constructed so as to (1) obtain ~~and encrypt~~ a date/time stamp in response to certain required information about the entity proposing to carry out the electronic transaction, and (2) generate a time-limited personal identification number (an "ePIN") by encrypting said date/time stamp and said certain required information, said certain required information including at least an account number ~~and~~ or a private personal identification number representing said entity;

(b) said entity supplies said certain required information to said computer program and in response said computer program ~~generates~~ obtains a date/time stamp ~~and encrypts~~ from a time source and generates an ePIN comprising said date/time stamp and said supplied certain required information;

(c) said ePIN is ~~encrypted date/time stamp and said encrypted certain required information are~~ transmitted to and received by said bank or a validating party representing said bank;

(d) said receiving bank or validating party decrypts said received ePIN to derive said ~~encrypted~~ date/time stamp and said supplied ~~received encrypted~~ certain required information;

(e) said receiving bank or validating party (1) compares said decrypted certain required information with previously recorded information in the possession of said bank or validating party to verify that the entity initiating the proposed transaction is an authorized entity and (2) ~~also compares the transaction time represented by said decrypted date/time stamp with the time of its receipt by said bank or validating party to determine if the difference, if any, between said times is within a predetermined time limit; and~~ also determines from said decrypted time stamp if the proposed transaction meets a predetermined time limit; and

(f) depending on the determination made in steps (e)(1) and (e)(2), said bank or validating party communicates either a validation or rejection of the proposed transaction to the entity who initiated the proposed credit card transaction.

28. (currently amended) A method according to claim 27 wherein in step (c) said ~~encrypted date/time stamp and encrypted certain required information are~~ ePIN is transmitted to and received by said validating party, ~~the steps in (e)~~ steps (e)(1) and (e)(2) are carried out by the validating party, and in step (f) the validating party communicates said validation or rejection of the proposed transaction to said bank.

29. (New) A method for conducting credit card transactions so as to guard against fraud, said method comprising steps as follows:

(a) a credit card user who proposes to carry out a credit card transaction with a credit card issuer or a third party vendor initiates the transaction by accessing a computer program supplied by the credit card issuer or a party acting on behalf of said credit card issuer that is constructed

so as to (1) obtain a date/time stamp from a time source and (2) generate an encrypted ePIN comprising said date/time stamp and certain required credit card information identifying a credit card user;

(b) said credit card user causes said computer program to generate an ePIN characterized by and comprising in encrypted form (1) credit card information provided by said user and (2) a date/time stamp obtained by said computer program in response to accessing of said computer program by said credit card user;

(c) said ePIN is transmitted directly or via a third party vendor to a validating system authorized to validate credit card transactions on behalf of said credit card issuer;

(d) said validating system decrypts said ePIN to derive the time represented by the decrypted date/time stamp and said credit card provided by said user;

(e) said validating system (1) compares said decrypted credit card information with previously recorded user information to verify that the user initiating the proposed transaction is an authorized credit card user and (2) determines from the decrypted date/time stamp whether the proposed transaction is within a predetermined time limit; and

(f) depending on the determinations made in foregoing steps (e)(1) and (e)(2), the validating system communicates either a validation or rejection of the proposed transaction to the credit card issuer and the party who initiated the proposed credit card transaction, and also to the third party vendor, if any.

30. (New) A method according to claim 29 wherein said ePIN comprises in encrypted form a credit card number and also a non-public personal identification code.

31. (New) A method according to claim 29 wherein step (c) also includes transmitting to the validating system other non-encrypted information relating to the identity of the party who initiates the transaction and/or to the subject matter of the transaction.

32. (New) A method according to claim 4 wherein said computer program is installed on a personal computer containing a browser, and said encrypted personal identification number is transmitted to said authorized party via the internet using said browser.

33. (New) A method according to claim 11 wherein said validating system receives said time-limited personal identification number via the internet.

34. (New) A method according to claim 20 wherein said computer program is installed on a personal computer and said encrypted personal identification number is transmitted from said computer via said vendor to said party authorized by the credit card issuer to validate proposed credit card transactions.